WHAT IS CLAIMED IS:

1. A method of archiving encryption keys used for encrypting information in a network, comprising:

collecting one or more encryption keys generated at at least one node in said network;

transmitting the one or more collected encryption keys to a key archive; and

storing said collected encryption keys in a database of said key archive.

2. The method of claim 1, further comprising:

time-stamping the one or more collected encryption keys.

3. The method of claim 1, further comprising:

tagging the one or more collected encryption bits with an identifier identifying a link of said network.

4. The method of claim 3, wherein said link of said network employed at least one of the collected encryption keys for encrypting data.

5. The method of claim 1, further comprising:

encrypting said collected encryption keys before transmitting said keys to said key archive.

6. The method of claim 1, further comprising:

digitally signing said collected encryption keys before transmitting said keys to said key archive.

7. A method of archiving encryption keys used for encrypting information in a network, comprising:

receiving encryption keys generated at a plurality of nodes in a network; and

storing said received encryption keys in an encryption key archive.

8. The method of claim 7, further comprising:

determining whether at least one of said encryption keys satisfies given standards.

9. The method of claim 8, further comprising:

notifying an entity if at least one of said encryption keys does not satisfy said given standards.

10. The method of claim 8, wherein said step of determining further comprises:

statistically analyzing at least one of said encryption keys.

11. The method of claim 10, wherein said step of statistically analyzing further comprises:

performing a correlation analysis to determine whether at least one of said encryption keys correlates with a specified parameter.

12. A computer-readable medium containing instructions for controlling at least one processor to perform a method of archiving encryption keys used for encrypting information in a network, the method comprising:

obtaining encryption keys generated at a plurality of nodes in a network; and

storing said received encryption keys in a database of an encryption key archive.

13. The computer-readable medium of claim 12, the method further comprising:

determining whether at least one of said encryption keys satisfies given standards.

14. The computer-readable medium of claim 13, the method further comprising:

notifying an entity if at least one of said encryption keys does not satisfy said given standards.

15. The computer-readable medium of claim 13, wherein said step of determining further comprises:

statistically analyzing at least one of said encryption keys.

16. The method of claim 15, wherein said step of statistically analyzing further comprises:

performing a correlation analysis to determine whether at least one of said encryption keys correlates with a specified parameter.

17. An encryption key archive, comprising:

a memory configured to store instructions; and

at least one processor configured to execute the instructions to:

receive encryption keys from a plurality of nodes in a network, and

store said received encryption keys in a database associated with said encryption key archive.

18. A system for archiving encryption keys used for encrypting information in a network, comprising:

means for collecting one or more encryption keys generated at at least one node in said network;

means for transmitting the one or more collected encryption keys to a key archive; and

means for storing said collected encryption keys in a database of said key archive.

19. A method of auditing encryption keys used for encrypting information in a network, comprising:

collecting one or more encryption keys generated at a node for encrypting data;

providing the one or more collected encryption keys to a key archive;

storing said collected encryption keys in a database of said key archive; and

determining whether at least one of said one or more collected keys satisfies given standards.

20. The method of claim 19, further comprising:

notifying an entity if said one or more collected keys does not satisfy said given standards.

21. The method of claim 19, wherein said step of determining further comprises:

statistically analyzing at least one of said one or more collected keys.

22. The method of claim 21, wherein said step of statistically analyzing further comprises:

performing a correlation analysis to determine whether at least one of said one or more collected keys correlates with a specified parameter.

23. A computer-readable medium containing instructions for controlling at least one processor to perform a method of auditing encryption keys used for encrypting information in a network, the method comprising:

receiving one or more encryption keys;

providing the one or more received encryption keys to a key archive; and

determining whether at least one of said one or more received keys satisfies given standards.

24. The computer-readable medium of claim 23, the method further comprising:

notifying an entity if said one or more received keys does not satisfy said given standards.

25. The computer-readable medium of claim 23, wherein said step of determining further comprises:

statistically analyzing at least one of said one or more received keys.

26. The computer-readable medium of claim 25, wherein said step of statistically analyzing further comprises:

performing a correlation analysis to determine whether at least one of said one or more received keys correlates with a specified parameter.

27. An encryption key archive, comprising:

a memory configured to store instructions and encryption keying bits; and

at least one processor configured to execute the instructions to:

receive one or more encryption keying bits generated at a node for encrypting data, and

statistically analyze at least one of said one or more keying bits.

28. A data structure encoded on a computer readable medium, comprising:

a plurality of encryption key bits received from a plurality of nodes in a network.

data indicating parameters associated with nodes employing cryptographic techniques in said network.

29. The data structure of claim 28, wherein said parameters indicate a number of indecipherable messages transmitted from each of said nodes.

30. The data structure of claim 28, wherein said parameters indicate a total number of messages transmitted from each of said nodes.

31. The data structure of claim 28, wherein said parameters indicate a number of failures associated with validations performed on said encryption key bits.

32. A method of transmitting encryption keys used for encrypting information at a node in a network to a key archive, comprising:

collecting one or more encryption keys generated at the node; and

transmitting the one or more encryption keys to the key archive.

33. A system for archiving encryption keys used for encrypting information in a network, comprising:

a plurality of nodes configured to:

collect one or more encryption keys generated at each node, and

transmit the one or more collected encryption keys to a key archive for storage in a database associated with the key archive, and

a key archive configured to:

receive encryptions keys transmitted from nodes in the network,

store the encryption keys in a database of the key archive.